AN ATTACK ON A KEY EXCHANGE PROTOCOL BASED ON MAX-TIMES AND MIN-TIMES ALGEBRAS

I. M. BUCHINSKIY, M. V. KOTOV, AND A. V. TREIER

Abstract. In this paper, we examine one of the public key exchange protocols proposed in [11] which uses max-times and min-times algebras. We discuss properties of powers of matrices over these algebras and introduce a fast attack on this protocol.

1. Introduction

In [28] Stickel generalized the well-known Diffie–Hellman key exchange method [8] to non-Abelian groups. The underlying algebraic structures of the proposed schemes were groups of invertible matrices over a finite field. Shpilrain [27] showed that Stickel's schemes were vulnerable to linear algebra attacks. Also, it is worth mentioning that in [22] Miasnikov and Roman'kov proposed a quite general linear decomposition attack on several group-based cryptosystems, which is also applicable to Stickel's schemes. To prevent linear algebra attacks, Grigoriev and Shpilrain [14] proposed a key-exchange protocol based on a min-plus matrix algebra. In [17] Kotov and Ushakov analyzed this protocol and suggested an attack on it. The key point of this attack is the fact that sequences of powers of matrices over a min-plus matrix algebra often display some patterns. Also, in [17] an attack on the same protocol with different restrictions on parameters was suggested. These protocol and attacks also were analyzed by Muanalifah and Sergeev in [20].

Grigoriev and Shpilrain in [15] offered two new key-exchange protocols based on tropical matrix algebras. They suggested using semidirect products to destroy patterns of sequences of powers of matrices which were exploited in the attacks on their first protocol. Three different approaches to attack one of these protocols were proposed. Isaac and Kahrobaei [16] used the property of a sequence of matrices to be almost linear periodic. Rudy and Monico [25] exploited the fact that the sequences of matrices appearing in the protocol are monotonically decreasing. This made it possible to apply a binary search. The attack suggested by Muanalifah and Sergeev in [21] is based on the solution of the tropical discrete logarithm problem.

Also, a series of key-exchange schemes based on max-plus algebras was proposed in the paper [12] by Durcheva and Trendafilov. In [1] Ahmed, Pal, and Mohan combined the techniques from the aforementioned papers and showed that all these protocols in this series are insecure.

Durcheva in [11] generalized the idea from [18] to use a two-sided action based on semirings and proposed a key exchange protocol that uses pairs of dual tropical structures. Two practical realizations were suggested: the first one is based on max-plus and min-plus algebras, and the second one is based on max-times and min-times matrix algebras. Subsequently, these two protocols were used as a part

of an encryption scheme in [10], and as a part of a distributed secure multicast protocol in [9].

The max-plus and min-plus realization of the protocol was analyzed by Ahmed, Pal, and Mohan in [1], where they showed that this protocol is insecure.

There is no known attack on the max-times and min-times realization. Note that the security of this protocol is based on the fact that there is no technique to solve systems of equations over max-times and min-times algebras. The main purpose of this article is to study sequences of powers of matrices over these algebras and propose a successful attack on this protocol.

For more information on non-commutative cryptography see [23].

The remainder of this paper is structured into five parts. In Section 2 we discuss tropical algebras, matrices, and polynomials over tropical algebras. In Section 3 we give the description of the protocol from [11] and discuss some issues of this description. In Section 4 we study the behavior of sequences of powers of matrices over max-times and min-times algebras. In Section 5 we introduce an attack on the protocol, give examples of how the attack works, and give the results of tests we ran. The final section offers a conclusion of our work.

2. Max-times and min-times algebras

In this section, we discuss tropical algebraic structures paying attention to max-times and min-times algebras, and define matrices and polynomials over tropical structures.

In this paper, we denote the set of non-negative real numbers by $\mathbb{R}_{\geqslant 0}$, the set of non-negative integers by $\mathbb{Z}_{\geqslant 0}$, and the set of positive integers by $\mathbb{Z}_{>0}$.

The *max-plus algebra* is the set $\mathbb{R} \cup \{-\infty\}$ equipped with the operations $x \oplus y = \max(x, y)$ and $x \otimes y = x + y$. The *min-plus algebra* is the set $\mathbb{R} \cup \{\infty\}$ equipped with the operations $x \oplus y = \min(x, y)$ and $x \otimes y = x + y$. These two algebras are known as tropical algebras. These algebras are semirings, which means they are similar to rings, but without the requirement that each element must have an additive inverse. Moreover, they are idempotent and commutative.

The tropical algebras have been widely studied and have a lot of applications. For more information, we refer the reader to [4] and [19].

One can also consider other algebraic structures in which one of the operations is min or max. Sometimes these algebras are also called tropical. For example, some researchers studied min-times and max-times algebras, where one of the operations is the multiplication of numbers and the other is either min or max [26, 29, 11]. Also, structures with both operations min and max were also considered [7, 13]. In [11] two different algebras are used simultaneously: one of the algebras has min, and the other has max.

In the remainder of this paper, we will use the max-times and min-times algebras, so we recall their definitions. The domain of the *max-times* algebra is $\mathbb{R}_{\geqslant 0} \cup \{\infty\}$, and the operations are

$$x \oplus y = \max(x, y) \quad \text{and} \quad x \otimes y = \begin{cases} 0 & \text{if } x = 0 \text{ or } y = 0, \\ x \cdot y & \text{otherwise.} \end{cases}$$

The domain of the *min-times* algebra is $\mathbb{R}_{\geqslant 0} \cup \{\infty\}$ and the operations are

$$x \oplus y = \min(x, y) \quad \text{and} \quad x \otimes y = \begin{cases} \infty & \text{if } x = \infty \text{ or } y = \infty, \\ x \cdot y & \text{otherwise.} \end{cases}$$

Since the max-times and max-times algebras are commutative idempotent semirings, then the following identities hold:

(1) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$,
(2) $o \oplus a = a \oplus o = a$,
(3) $a \oplus b = b \oplus a$,
(4) $(a \otimes b) \otimes c = a \otimes (b \otimes c)$,
(5) $e \otimes a = a \otimes e = a$,
(6) $a \otimes b = b \otimes a$,
(7) $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$,
(8) $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$,
(9) $o \otimes a = a \otimes o = o$,
(10) $a \oplus a = a$,

where o is 0 for the max-times algebra and is ∞ for the min-times algebra, and e is 1.

Let $\mathcal{S} = \langle S, \oplus, \otimes \rangle$ be a semiring. The set of all $n \times n$ matrices $\mathrm{Mat}_n(\mathcal{S})$ with entries in S can be equipped with addition $\oplus$ and multiplication $\otimes$ as well:

$$(a_{ij}) \oplus (b_{ij}) = (a_{ij} \oplus b_{ij}),$$

$$(a_{ij}) \otimes (b_{ij}) = (a_{i1} \otimes b_{1j} \oplus \cdots \oplus a_{in} \otimes b_{nj}).$$

For example, let's consider two matrices over max-times algebra:

$$A = \begin{pmatrix} 1 & 2 \\ 0 & \infty \end{pmatrix}, B = \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix}.$$

Then the product of these matrices is

$$A \otimes B = \begin{pmatrix} 1 & 2 \\ 0 & \infty \end{pmatrix} \otimes \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix} = \begin{pmatrix} 1 \otimes 3 \oplus 2 \otimes 5 & 1 \otimes 4 \oplus 2 \otimes 0 \\ 0 \otimes 3 \oplus \infty \otimes 5 & 0 \otimes 4 \oplus \infty \otimes 0 \end{pmatrix} = \begin{pmatrix} 3 \oplus 10 & 4 \oplus 0 \\ 0 \oplus \infty & 0 \oplus 0 \end{pmatrix} = \begin{pmatrix} 10 & 4 \\ \infty & 0 \end{pmatrix}.$$

Multiplying a matrix by a scalar is just multiplying by the corresponding scalar matrix.

The obtained set of matrices also in an idempotent semiring. In other words, the following identities are true:

(1) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$,
(2) $O \oplus A = A \oplus O = A$,
(3) $A \oplus B = B \oplus A$,
(4) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$,
(5) $E \otimes A = A \otimes E = A$,
(6) $A \otimes (B \oplus C) = (A \otimes B) \oplus (A \otimes C)$,
(7) $(A \oplus B) \otimes C = (A \otimes C) \oplus (B \otimes C)$,
(8) $O \otimes A = A \otimes O = O$,
(9) $A \oplus A = A$,

where for the max-times algebra

$$O = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad E = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

and for the min-times algebra

$$O = \begin{pmatrix} \infty & \infty & \cdots & \infty \\ \infty & \infty & \cdots & \infty \\ \vdots & \vdots & \ddots & \vdots \\ \infty & \infty & \cdots & \infty \end{pmatrix} \quad \text{and} \quad E = \begin{pmatrix} 1 & \infty & \cdots & \infty \\ \infty & 1 & \cdots & \infty \\ \vdots & \vdots & \ddots & \vdots \\ \infty & \infty & \cdots & 1 \end{pmatrix}.$$

We denote an element of the semiring a raised to the n-th power by $a^{\otimes n}$.

It is possible to define the set of polynomials over $\mathcal{S}$. Also, let $A \in \mathrm{Mat}_n(\mathcal{S})$ and $p(x) = \bigoplus_{i=0}^{d} p_i \otimes x^{\otimes i}$, then we denote the matrix $\bigoplus_{i=0}^{d} p_i \otimes A^{\otimes i}$ by $p(A)$.

In this paper, for a matrix A, we will often use a_{ij} to refer to the element at the i-th row and j-th column of the matrix A.

3. The protocol

In this section, we discuss the key exchange protocol proposed in [11].

Let $\mathcal{R}_{\max,\times} = \langle \mathbb{R}_{\geqslant 0} \cup \{\infty\}, \boxplus, \boxtimes \rangle$ and $\mathcal{R}_{\min,\times} = \langle \mathbb{R}_{\geqslant 0} \cup \{\infty\}, \oplus, \otimes \rangle$ be the max-times and min-times algebras respectively.

The following protocol was proposed in [11].

Protocol 1. Alice and Bob agree on three matrices $M, N, X \in \mathrm{Mat}_n(\mathbb{Z}_{\geqslant 0})$.

(1) Alice chooses polynomials $p(x) \in \mathcal{R}_{\max,\times}[x]$ and $t(x) \in \mathcal{R}_{\min,\times}[x]$ and computes $A = p(M) \boxtimes X \otimes t(N)$. The pair $(p(x), t(x))$ is her secret key, and the matrix A is her public key.
(2) Bob chooses polynomials $q(x) \in \mathcal{R}_{\max,\times}[x]$ and $r(x) \in \mathcal{R}_{\min,\times}[x]$ and computes $B = q(M) \boxtimes X \otimes r(N)$. The pair $(q(x), r(x))$ is Bob's secret key, and the matrix B is Bob's public key.
(3) Alice computes $k_A = p(M) \boxtimes B \otimes t(N)$.
(4) Bob computes $k_B = q(M) \boxtimes A \otimes r(N)$.

In the original paper [11] and the subsequent papers [10, 9], the authors claimed that Alice and Bob shared the same key. Unfortunately, this is not true. First, in general, $(M \boxtimes X) \otimes N \neq M \boxtimes (X \otimes N)$. For example, let

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad N = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix},$$

then

$$(M \boxtimes X) \otimes N = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, \quad M \boxtimes (X \otimes N) = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}.$$

Therefore the expression $M \boxtimes X \otimes N$ is not well-defined, and parentheses must be written to define an order of operations. In the source code of the implementation of the protocol [10], the following order of operations is implicitly used: $A = (p(M) \boxtimes X) \otimes t(N)$, $B = (q(M) \boxtimes X) \otimes r(N)$, $k_A = (p(M) \boxtimes B) \otimes t(N)$, and $k_B = (q(M) \boxtimes A) \otimes r(N)$. Thus, we will use this order in the remainder of the paper.

Second, in general,

$$(p(M) \boxtimes ((q(M) \boxtimes X) \otimes r(N))) \otimes t(N) \neq (q(M) \boxtimes ((p(M) \boxtimes X) \otimes t(N))) \otimes r(N). \quad (1)$$

Indeed, let

$$M = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}, \quad X = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}, \quad N = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

and $p(x) = t(x) = r(x) = x$, $q(x) = x^{\otimes 2}$. Then

$$A = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix}, B = \begin{pmatrix} 6 & 6 \\ 9 & 9 \end{pmatrix}, k_A = \begin{pmatrix} 12 & 12 \\ 27 & 27 \end{pmatrix}, k_B = \begin{pmatrix} 9 & 9 \\ 27 & 27 \end{pmatrix}.$$

Hence this protocol cannot be implemented correctly. Our experiments show that the inequality (1) holds only for about 2% of randomly generated instances of the protocol, where the size of the matrices is 10, the coefficients are in $[0, 1000]$, and the degrees of the polynomials do not exceed 10. Therefore the description is not completely wrong. So, before choosing the polynomials Alice and Bob should agree on two sets of polynomials $P \subseteq \mathcal{R}_{\max,\times}[x]$ and $R \subseteq \mathcal{R}_{\min,\times}[x]$ such that the following equality is true for all $p(x), q(x) \in P$ and $r(x), t(x) \in R$:

$$(p(M)\boxtimes((q(M)\boxtimes X)\otimes r(N)))\otimes t(N) = (q(M)\boxtimes((p(M)\boxtimes X)\otimes t(N)))\otimes r(N). \quad (2)$$

So, the following description of the protocol should be considered.

Protocol 2. Alice and Bob agree on matrices $M, X, N \in \mathrm{Mat}_n(\mathbb{Z}_{\geqslant 0})$ and two sets of polynomials $P \subseteq \mathcal{R}_{\max,\times}[x]$ and $R \subseteq \mathcal{R}_{\min,\times}[x]$ such that the equality (2) is true for all $p(x), q(x) \in P$ and $r(x), t(x) \in R$.

(1) Alice chooses two polynomials $p(x) \in P$ and $t(x) \in R$ and computes $A = (p(M) \boxtimes X) \otimes t(N)$. The pair $(p(x), t(x))$ is her secret key, and the matrix A is her public key.
(2) Bob chooses two polynomials $q(x) \in P$ and $r(x) \in R$ and computes $B = (q(M)\boxtimes X\otimes)r(N)$. The pair $(q(x), r(x))$ is Bob's secret key, and the matrix B is Bob's public key.
(3) Alice computes $k_A = (p(M) \boxtimes B) \otimes t(N)$.
(4) Bob computes $k_B = (q(M) \boxtimes A) \otimes r(N)$.

The shared common secret key is $k_A = k_B$. Now k_A and k_B are truly equal because of (2).

There are at least two strategies to break the protocol. The first one is to find two polynomials $p'(x) \in P$ and $t'(x) \in R$ such that $A = (p'(M) \boxtimes X) \otimes t'(N)$. The second strategy is to find four polynomials $p'(x), q'(x) \in \mathcal{R}_{\max,\times}[x]$ and $t'(x), r'(x) \in \mathcal{R}_{\min,\times}[x]$ such that $A = (p'(M) \boxtimes X) \otimes t'(N)$, $B = (q'(M) \boxtimes X) \otimes r'(N)$, and $(p'(M) \boxtimes B) \otimes t'(N) = (q'(M) \boxtimes A) \otimes r'(N)$. The second one is useful when we have no information about P and R.

4. Behavior of matrix sequences over max-times and min-times algebras

In this section, we study behavior of sequences $\{M^{\boxtimes n}\}_{n=0}^{\infty}$, $\{N^{\otimes n}\}_{n=0}^{\infty}$, $\{M^{\boxtimes n} \boxtimes X\}_{n=0}^{\infty}$, $\{X \otimes N^{\otimes n}\}_{n=0}^{\infty}$, $\{p_0 \boxplus p_1 \boxtimes M \boxplus \ldots \boxplus p_n \boxtimes M^{\boxtimes n}\}_{n=0}^{\infty}$, and $\{r_0 \oplus r_1 \otimes N \oplus \ldots \oplus r_n \otimes N^{\otimes n}\}_{n=0}^{\infty}$, where X, M and N are matrices, and p_i and r_j are numbers.

In this and in the following sections, for a matrix A, $\min(A)$ means $\min_{i,j}(a_{ij})$, and $\max(A)$ means $\max_{i,j}(a_{ij})$. Also, we will use the following order of matrices: $A \geqslant B$ iff $a_{ij} \geqslant b_{ij}$ for all i and j.

Remark 1. Let $N \in \mathrm{Mat}_n(\mathbb{Z}_{\geqslant 0})$, and one of the entries of N be 0. Then $N^{\otimes 2}$ has a row and a column filled with 0, and $N^{\otimes 3}$ is the matrix filled with 0. Thus, if $t(x)$ is not linear, then $(p(M) \boxtimes X) \otimes t(N)$ is the matrix filled with 0. If one of the coefficients of $x^{\otimes i}$, $i > 0$, of $t(x)$ is 0, then $t(N)$ also is the matrix filled with 0.

Hence, to avoid trivial keys, Alice and Bob should not use N, $t(x)$, and $r(x)$ with zeros.

Remark 2. Let $M \in \mathrm{Mat}_n(\mathbb{Z}_{\geqslant 0})$. If the number of the entries of M that are equal to 0 is small, then often a power of the matrix M does not have zeros because every time we compute the maximum of products. For example,

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad A^{\boxtimes 4} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Based on Remark 1 and Remark 2, we will assume that matrices do not have zero entries in order to make our reasoning easier.

Remark 3. Let $X, Y \in \mathrm{Mat}_n(\mathbb{Z}_{>0})$. Then $X \boxtimes Y \geqslant X$ and $X \boxtimes Y \geqslant Y$. Indeed,

$$X \boxtimes Y = (x_{i1} \boxtimes y_{1j} \boxplus \cdots \boxplus x_{in} \boxtimes y_{nj}) = \\ \max(x_{i1}y_{1j}, \ldots, x_{in}y_{nj}) \geqslant \max(x_{i1}, \ldots, x_{in}) \geqslant (x_{ij}) = X.$$

The second inequality can be proven in the same way.

Remark 4. Let $M \in \mathrm{Mat}_n(\mathbb{Z}_{>0})$, $X \in \mathrm{Mat}_n(\mathbb{Z}_{\geqslant 0})$. The sequences $\{M^{\boxtimes n}\}_{n=0}^{\infty}$ and $\{M^{\boxtimes n} \boxtimes X\}_{n=0}^{\infty}$ are not decreasing.

Indeed, using the previous remark, we obtain

$$M^{\boxtimes n+1} = M \boxtimes M^{\boxtimes n} \geqslant M^{\boxtimes n},$$
$$M^{\boxtimes n+1} \boxtimes X = M \boxtimes (M^{\boxtimes n} \boxtimes X) \geqslant M^{\boxtimes n} \boxtimes X.$$

For randomly generated matrices, we can expect that these sequences are increasing because the number of entries that are equal to 1 is small.

Remark 5. Let $H, G \in \mathrm{Mat}_n(\mathbb{Z}_{\geqslant 0})$, then $\min(H \otimes G) \geqslant \min(H) \cdot \min(G)$. Indeed,

$$\min(H \otimes G) = \min_{i,j}(\bigoplus_k h_{ik} \otimes g_{kj}) = \min_{i,j}(\min_k(h_{ik}g_{kj})) = \min_{i,j,k}(h_{ik}g_{kj}) \geqslant \\ \min_{i,j}(h_{ij}) \cdot \min_{i,j}(g_{ij}) = \min(H) \cdot \min(G).$$

Remark 6. Let $N \in \mathrm{Mat}_n(\mathbb{Z}_{>0})$, $Y \in \mathrm{Mat}_n(\mathbb{Z}_{\geqslant 0})$, then $\min(N^{\otimes n+1}) \geqslant \min(N^{\otimes n})$ and $\min(Y \otimes N^{\otimes n+1}) \geqslant \min(Y \otimes N^{\otimes n})$. This immediately follows from the previous remark:

$$\min(N^{\otimes n+1}) = \min(N^{\otimes n} \otimes N) \geqslant \min(N^{\otimes n}) \cdot \min(N) \geqslant \min(N^{\otimes n}).$$

The second inequality can be proven in the same way.

Remark 7. Let $H, G \in \mathrm{Mat}_n(\mathbb{Z}_{\geqslant 0})$, then $\min(H \oplus G) \geqslant \min(\min(H), \min(G))$. Indeed,

$$\min(H \oplus G) = \min_{i,j}(\min(h_{ij}, g_{ij})) \geqslant \\ \min_{i,j}(\min(\min(H), \min(G)) = \min(\min(H), \min(G)).$$

Remark 8. Let $M \in \mathrm{Mat}_n(\mathbb{Z}_{>0})$, and $p(x) \in \mathcal{R}_{\max,\times}[x]$. We can expect that often

$$p(M) = p_d \boxtimes M^{\boxtimes d}, \tag{3}$$

where $d = \deg(p(x))$. Indeed, let us consider the sum of two consecutive monomials: $p_{i+1} \boxtimes M^{\boxtimes i+1} \boxplus p_i \boxtimes M^{\boxtimes i} = (p_{i+1} \boxtimes M \boxplus p_i \boxtimes E) \boxtimes M^{\boxtimes i}$. The condition $p_{i+1} \boxtimes M \boxplus$

$p_i \boxtimes E = p_{i+1} \boxtimes M$ means that $p_{i+1} m_{jj} \geqslant p_i$ for all $j \in [1, n]$. Since the coefficients of polynomials and the entries of matrices are chosen from an interval $[0, B]$, then we can expect that the probability of this event is high. To check this, we randomly generated pairs of a matrix and a polynomial, where the size of the matrices is 10, the coefficients and the entries are in $[0, 1000]$, and the degrees of the polynomials are in $[5, 20]$. The equality (3) holds for about 99.9% of the generated pairs.

Remark 9. Let $N \in \mathrm{Mat}_n(\mathbb{Z}_{>0})$. Our experiments show that a polynomial $r(x) \in \mathcal{R}_{\min,\times}[x]$ often is equal to its beginning:

$$r(N) = r_0 \oplus r_1 \otimes N \oplus \ldots \oplus r_{d_0} \otimes N^{\otimes d_0}, \tag{4}$$

where $d_0 < d = \deg(r(x))$. We randomly generated pairs of a matrix and a polynomial, where the size of the matrices is 10, the coefficients and the entries are in $[0, 1000]$, and the degrees of the polynomials is 20. For about 99% of the generated pairs and $d_0 = 10$, the equality (4) holds. If the coefficients and the entries are from $[0, 10000]$, then the rate is about 99.9%.

Remark 10. A sequence of matrices $\{A_i\}_{i=0}^{\infty}$ is called *almost linear periodic* if there exist a period ρ, a factor c, and a defect δ such that for all $i > \delta$ the following equation holds:

$$A_{i+\rho} = c + A_i.$$

For sequences of powers of a matrix over tropical algebras, this property is well studied [2, 5, 6, 24]. It is used in [16] to analyze the protocol from [15].

Since we study the max-times and min-times structures, there is an isomorphism, $x \mapsto e^x$, between max-plus and max-times algebras, and between min-plus and min-times algebras, we will consider the following property.

We say that a sequence of matrices $\{A_i\}_{i=0}^{\infty}$ is *almost multiplicatively periodic* if there exist a period ρ, a factor c and a defect δ such that for all $i > \delta$ the following equation holds:

$$A_{i+\rho} = c \cdot A_i.$$

Let's consider two examples.

$$A = \begin{pmatrix} 2 & 5 & 3 \\ 5 & 0 & 4 \\ 4 & 3 & 5 \end{pmatrix}, A^{\boxtimes 2} = \begin{pmatrix} 25 & 10 & 20 \\ 16 & 25 & 20 \\ 20 & 20 & 25 \end{pmatrix}, A^{\boxtimes 3} = \begin{pmatrix} 80 & 125 & 100 \\ 125 & 80 & 100 \\ 100 & 100 & 125 \end{pmatrix},$$

$$A^{\boxtimes 4} = \begin{pmatrix} 625 & 400 & 500 \\ 400 & 625 & 500 \\ 500 & 500 & 625 \end{pmatrix}, A^{\boxtimes 5} = \begin{pmatrix} 2000 & 3125 & 2500 \\ 3125 & 2000 & 2500 \\ 2500 & 2500 & 3125 \end{pmatrix} = 25 \cdot A^{\boxtimes 3},$$

$$A^{\boxtimes 6} = \begin{pmatrix} 15625 & 10000 & 12500 \\ 10000 & 15625 & 12500 \\ 12500 & 12500 & 15625 \end{pmatrix} = 25 \cdot A^{\boxtimes 4}.$$

$$B = \begin{pmatrix} 5 & 3 & 3 \\ 4 & 3 & 1 \\ 2 & 2 & 5 \end{pmatrix}, B^{\otimes 2} = \begin{pmatrix} 6 & 6 & 3 \\ 2 & 2 & 3 \\ 8 & 6 & 2 \end{pmatrix}, B^{\otimes 3} = \begin{pmatrix} 6 & 6 & 6 \\ 6 & 6 & 2 \\ 4 & 4 & 6 \end{pmatrix},$$

$$B^{\otimes 4} = \begin{pmatrix} 12 & 12 & 6 \\ 4 & 4 & 6 \\ 12 & 12 & 4 \end{pmatrix}, B^{\otimes 5} = \begin{pmatrix} 12 & 12 & 12 \\ 12 & 12 & 4 \\ 8 & 8 & 12 \end{pmatrix} = 2 \cdot B^{\otimes 3},$$

$$B^{\otimes 6} = \begin{pmatrix} 24 & 24 & 12 \\ 8 & 8 & 12 \\ 24 & 24 & 8 \end{pmatrix} = 2 \cdot B^{\otimes 4}.$$

We performed the following experiments. We randomly generated matrices of size 10×10, the entries of them were chosen from an interval $[0, 1000]$, and computed the sequences $\{A^{\otimes i}\}_{i=1}^{1000}$. We checked the following restricted property: if there are a number ρ, a factor c and a defect $\delta < 100$ such that for all $\delta < i \leqslant 1000$ the following equations hold:

$$A^{\otimes i+\rho} = c \cdot A^{\otimes i}.$$

Also, we did the same for $\{A^{\boxtimes i}\}_{i=1}^{1000}$. It turned out that for the max-times case the restricted property is true for 99.6% of the randomly generated matrices, and for the min-times case the restricted property is true for 97.9% for the randomly generated matrices.

Also, for the same set of parameters, our experiments show the following properties of the distributions of δ and ρ. For the min-times case, average δ is 11.51, average ρ is 2.24, median δ is 7, median ρ is 2, maximal δ is 242, and maximal ρ is 8. For the max-times case, average δ is 26.42, average ρ is 2.13, median δ is 11, and median ρ is 2, maximal δ is 772, and maximal ρ is 8. (We counted only those matrices for which δ and ρ were found.)

Remark 11. If a matrix A has this property, then $p(A) = \bigoplus_{i=0}^{n} p_i \otimes A^{\otimes i}$ is equal to $\bigoplus_{i=0}^{n'} p'_i \otimes x^{\otimes i}$, where $n' \leqslant \delta(A) + \rho(A)$. The same is true for $t(N) = \bigoplus_{i=0}^{n} t_i \otimes N^{\otimes i}$.

5. Attack

In this section, we present our attack as well as the results of our experiments.

We will try to find polynomials $p'(x)$, $q'(x)$, $t'(x)$, and $r'(x)$ such that

$$A = (p'(M) \boxtimes X) \otimes t'(N), B = (q'(M) \boxtimes X) \otimes r'(N), \text{ and}$$
$$(p'(M) \boxtimes B) \otimes t'(N) = (q'(M) \boxtimes A) \otimes r'(N).$$

Let's describe how we will try to find $p'(x)$ and $t'(x)$. The procedure to find $q'(x)$ and $r'(x)$ is the same.

Taking into account Remark 8, we can try to find the polynomial $p'(x)$ of the form $p_i \boxtimes x^{\boxtimes i}$. Because

$$((p_i \boxtimes M^{\boxtimes i}) \boxtimes X) \otimes t'(N) = (M^{\boxtimes i} \boxtimes X) \otimes (p_i \otimes t'(N)), \tag{5}$$

it is enough to find the polynomial $p'(x)$ of the form $x^{\boxtimes i}$. In order to do this, we will enumerate degrees i from 0 to a bound u_p. We will describe how to find this bound below.

Next, taking into account Remark 9, we will find $t'(x)$ of the form $t'(x) = t_0 \oplus t_1 \otimes x \oplus t_2 \otimes x^{\otimes 2} \oplus \ldots \oplus t_j \otimes x^{\otimes j}$ trying degrees j from 0 to a bound u_t. We will describe how to find this bound below as well.

Let $p'(x)$ be known. Since $(p'(M) \boxtimes X) \otimes t'(X) = A$, we have

$$(p'(M) \boxtimes X) \otimes \left(\bigoplus_{k=0}^{j} t_k \otimes N^{\otimes k} \right) = A.$$

Therefore,

$$\bigoplus_{k=0}^{j} t_k \otimes (p'(M) \boxtimes X) \otimes N^{\otimes k} = A.$$

Let $C_k = (p'(M) \boxtimes X) \otimes N^{\otimes k}$. We have the following system of equations:

$$\min_k (t_k c_{klm}) = a_{lm}.$$

In other words,

$$\begin{array}{rcl} \min(t_0c_{011}, t_1c_{111}, \ldots, t_kc_{k11}) & = & a_{11}, \\ \min(t_0c_{012}, t_1c_{112}, \ldots, t_kc_{k12}) & = & a_{12}, \\ & \ldots & \\ \min(t_0c_{0nn}, t_1c_{1nn}, \ldots, t_kc_{knn}) & = & a_{nn}. \end{array}$$

If the system is solvable, then a solution to this system is

$$t_k = \begin{cases} \max_{l,m}(a_{lm}/c_{klm}) & \text{if this number is an integer,} \\ \infty & \text{otherwise.} \end{cases}$$

Next, since $A = (p'(M) \boxtimes X) \otimes t'(N)$, we have

$$\min(A) \geqslant \min(p'(M) \boxtimes X) \cdot \min(t'(N)) \geqslant \min(p'(M) \boxtimes X).$$

By Remark 4, the sequence $M^{\boxtimes i} \boxtimes X$ is not decreasing. Therefore, we can stop our search and say that our algorithm failed when

$$\min(M^{\boxtimes i} \boxtimes X) > \min(A).$$

Also, $\min((p'(M) \boxtimes X) \otimes t'(N)) = \min((p'(M) \boxtimes X) \otimes \left(\bigoplus_k t_k \otimes N^{\otimes k}\right)) = \min\left(\bigoplus_k (t_k \otimes (p'(M) \boxtimes X) \otimes N^{\otimes k})\right) = \min(\bigoplus_k ((p'(M) \boxtimes X) \otimes N^{\otimes k}))$.

By Remark 6 and 7, $\min(\bigoplus_k ((p'(M) \boxtimes X) \otimes N^{\otimes k})) \leqslant \min(p'(M) \boxtimes X) \otimes N^{\otimes j})$. Therefore we should search until

$$\min(p'(M) \boxtimes X) \otimes N^{\otimes j}) > \max(A).$$

Note that u_p and u_t can be found using the almost multiplicatively periodic property. We should check i while $i \leqslant \delta(M) + \rho(M)$ and check j while $j \leqslant \delta(N) + \rho(N)$. Indeed, if $i > \delta(M) + \rho(M)$, then $M^i = c \boxtimes M^{\boxtimes i'}$, where $i' \leqslant \delta(M) + \rho(M)$. Using 5, we obtain the result. The second inequality follows from Remark 11. Note that if we have reasonable enough bounds u_p and u_t we do not have to find these periods and defects before the loops, and can find them during the search process. To check the almost multiplicatively periodic property, we perform the element-by-element division M^i/M^k for $k < i$ and check if all the elements of the result matrix are the same.

Putting it together, we obtain the following procedure to find $p'(x)$ and $t'(x)$.

for $i = 0, 1, \ldots, u_p$ **do**
  if there exist $k < i$ and c s. t. $M^i/M^k = (c)$ **then**
    return FAIL
  end if
  $p'(x) \leftarrow x^{\boxtimes i}$
  if $\min(p'(M) \boxtimes X) > \min(A)$ **then**
    return FAIL
  end if
  for $j = 0, 1, \ldots, u_t$ **do**
    if there exist $k < j$ and c s. t. $N^j/N^k = (c)$ **then**
      break
    end if
    if $\min((p'(M) \boxtimes X) \otimes N^{\otimes j}) > \max(A)$ **then**
      break
    end if

$$t_j \leftarrow \begin{cases} \max(A/((M^{\boxtimes i} \boxtimes X) \otimes N^{\otimes j})) & \text{if this number is an integer,} \\ \infty & \text{otherwise.} \end{cases}$$

$t'(x) \leftarrow t'(x) \oplus t_j \otimes x^{\otimes j}$
if $(p'(M) \boxtimes X) \otimes t'(N) = A$ **then**
return $p'(x)$, $t'(x)$
end if
end for
end for
return FAIL

So, the attack looks like

(1) Find $p'(x)$ and $t'(x)$ using the algorithm described above.
(2) Find $q'(x)$ and $r'(x)$ using the algorithm described above.
(3) Check that $(p'(M) \boxtimes B) \otimes t'(N) = (q'(M) \boxtimes A) \otimes r'(N)$. If it is true, then return $K = (p'(M) \boxtimes B) \otimes t'(N)$. Otherwise, return FAIL.

Let's consider the example from [11].

$$M = \begin{pmatrix} 5 & 7 & 1 \\ 4 & 2 & 3 \\ 2 & 5 & 6 \end{pmatrix}, N = \begin{pmatrix} 2 & 1 & 3 \\ 7 & 5 & 4 \\ 3 & 1 & 9 \end{pmatrix}, X = \begin{pmatrix} 5 & 2 & 8 \\ 6 & 7 & 4 \\ 3 & 1 & 5 \end{pmatrix},$$

$$p(x) = x^{\boxtimes 3} \boxplus 5 \boxtimes x^{\boxtimes 2} \boxplus 10 \boxtimes x, t(x) = 3 \otimes x^{\otimes 2} \oplus x,$$

$$q(x) = x^{\boxtimes 2} \boxplus 5 \boxtimes x, r(x) = 10 \otimes x^{\otimes 4} \oplus x^{\otimes 2}.$$

The key is

$$K = \begin{pmatrix} 263424 & 125440 & 263424 \\ 188160 & 94080 & 188160 \\ 311040 & 155520 & 311040 \end{pmatrix}.$$

The attack finds the following $p'(x)$, $t'(x)$, $q'(x)$ and $r'(x)$:

$$p'(x) = x^{\boxtimes 3}, t'(x) = x, q'(x) = x^{\boxtimes 2}, r'(x) = x^{\otimes 2} \oplus 4.$$

For these polynomials, we have

$$(p'(M) \boxtimes B) \otimes t'(N) = (q'(M) \boxtimes A) \otimes r'(N) = K.$$

The described attack was implemented in Python and can be found in [3]. The tests were performed on the workstation of Omsk Regional Supercomputer Center of SB RAS with AMD EPYC 7502, 32 cores at 2.5GHz with 512GB of RAM, Ubuntu 20.04 Server. We generated 100 random instances for every set of parameters presented in Table 1.

6. Conclusion

In this paper, we showed that the protocol described in [11] is not correctly defined. We could have finished our analysis here, but using the implementation from [10], we suggested how the description of the protocol can be corrected. We analyzed the corrected protocol and showed that it is insecure. The success rate of our attack is 100%. Therefore using the max-times and min-times structures instead of the max-plus and min-plus structures does not make the protocol more secure. Our analysis can further be used to analyze other protocols based on max-times and min-times matrix algebras.

Size of matrices	Degrees of polynomials	Coefficients	Success Rate	Avg. Time
10	$[1, 10]$	$[1, 100]$	100%	0.51 sec
10	$[1, 10]$	$[1, 1000]$	100%	0.57 sec
10	$[1, 20]$	$[1, 100]$	100%	1.18 sec
10	$[1, 20]$	$[1, 1000]$	100%	1.02 sec
20	$[1, 10]$	$[1, 100]$	100%	7.07 sec
20	$[1, 10]$	$[1, 1000]$	100%	4.64 sec
20	$[1, 20]$	$[1, 100]$	100%	10.88 sec
20	$[1, 20]$	$[1, 1000]$	100%	9.60 sec
50	$[1, 10]$	$[1, 100]$	100%	186.27 sec
50	$[1, 10]$	$[1, 1000]$	100%	110.34 sec
50	$[1, 20]$	$[1, 100]$	100%	303.33 sec
50	$[1, 20]$	$[1, 1000]$	100%	234.78 sec

TABLE 1. Experimental results of the attack

FUNDING

The research was supported by Russian Scientific Foundation, project No. 22-11-20019.

REFERENCES

[1] K. Ahmed, S. Pal, and R. Mohan. A review of the tropical approach in cryptography. *Cryptologia*, pages 1–25, 2021.

[2] F. Baccelli, G. Cohen, G. Olsder, and J. Quadrat. *Synchronization and linearity: an algebra for discrete event systems*. John Wiley & Sons Ltd, 1992.

[3] I. Buchinskiy, M. Kotov, and A. Treier. The source code of the described attack. `https://github.com/mkotov/tropical2`.

[4] P. Butkovič. *Max-linear systems: theory and algorithms*. Springer Science & Business Media, 2010.

[5] G. Cohen, D. Dubois, J. Quadrat, and M. Viot. A linear-system-theoretic view of discrete-event processes and its use for performance evaluation in manufacturing. *IEEE transactions on Automatic Control*, 30(3):210–220, 1985.

[6] R. Cuninghame-Green. Lecture notes in economics and mathematical systems. In *Minimax algebra*, volume 166. Springer-Verlag New York, NY, USA, 1979.

[7] R. A. Cuninghame-Green. Minimax algebra and applications. *Fuzzy Sets and Systems*, 41(3):251–267, 1991.

[8] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[9] M. Durcheva and M. Ivanova. Key agreement protocol for distributed secure multicast for eAssessment. *International Journal on Information Technologies and Security*, 10(1):47–58, 2018.

[10] M. Durcheva and M. Rachev. A public key encryption scheme based on idempotent semirings. In *AIP Conference Proceedings*, volume 1690, page 060008. AIP Publishing LLC, 2015.

[11] M. I. Durcheva. An application of different dioids in public key cryptography. In *AIP Conference Proceedings*, volume 1631, pages 336–343. American Institute of Physics, 2014.

[12] M. I. Durcheva and I. D. Trendafilov. Public key cryptosystem based on max-semirings. In *AIP Conference Proceedings*, volume 1497, pages 357–364. American Institute of Physics, 2012.

[13] Y. Dvorzhetskiy and M. Kotov. Minimax algebraic structures. *Vestn. Omsk. Univ.*, Spec. Vol.: Combinatorial Methods of Algebra and Computational Complexity:130–136, 2008.

[14] D. Grigoriev and V. Shpilrain. Tropical cryptography. *Comm. Algebra*, 42(6):2624–2632, 2014.

[15] D. Grigoriev and V. Shpilrain. Tropical cryptography II: extensions by homomorphisms. *Comm. Algebra*, 47(10):4224–4229, 2019.
[16] S. Isaac and D. Kahrobaei. A closer look at the tropical cryptography. *International Journal of Computer Mathematics: Computer Systems Theory*, 6(2):137–142, 2021.
[17] M. Kotov and A. Ushakov. Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology*, 12(3):137–141, 2018.
[18] G. Maze, C. Monico, and J. Rosenthal. Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications*, 1(4):489–507, 2007.
[19] G. Mikhalkin. Tropical geometry and its applications. *arXiv preprint math/0601041*, 2006.
[20] A. Muanalifah and S. Sergeev. Modifying the tropical version of Stickel's key exchange protocol. *Applications of Mathematics*, 65(6):727–753, 2020.
[21] A. Muanalifah and S. Sergeev. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. *Communications in Algebra*, pages 1–19, 2021.
[22] A. G. Myasnikov and V. A. Roman'kov. A linear decomposition attack. *Groups Complexity Cryptology*, 7(1):81–94, 2015.
[23] A. G. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*, volume 177 of *Mathematical surveys and monographs*. American Mathematical Soc., 2011.
[24] K. Nachtigall and et al. Powers of matrices over an extremal algebra with applications to periodic graphs. *Mathematical Methods of Operations Research*, 46(1):87–102, 1997.
[25] D. Rudy and C. Monico. Remarks on a tropical key exchange system. *Journal of Mathematical Cryptology*, 15(1):280–283, 2021.
[26] Y. Shitov. A note on square roots of nonnegative matrices. *Linear Algebra and Its Applications*, 497:62–65, 2016.
[27] V. Shpilrain. Cryptanalysis of Stickel's key exchange scheme. In *International computer science symposium in Russia*, pages 283–288. Springer, 2008.
[28] E. Stickel. A new method for exchanging secret keys. In *Third International Conference on Information Technology and Applications (ICITA'05)*, volume 2, pages 426–430. IEEE, 2005.
[29] I. M. Sulandra and A. N. Isnia. On square roots of matrices over the max-time semiring $\mathbb{R}_+$. In *Journal of Physics: Conference Series*, volume 1872, page 012014. IOP Publishing, 2021.

I. M. Buchinskiy, Sobolev Institute of Mathematics of SB RAS, Omsk, Russia
Email address: buchvan@mail.ru

M. V. Kotov, Sobolev Institute of Mathematics of SB RAS, Omsk, Russia
Email address: matvej.kotov@gmail.com

A. V. Treier, Sobolev Institute of Mathematics of SB RAS, Omsk, Russia
Email address: alexander.treyer@gmail.com